

PAENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-162680

(43)Date of publication of application : 06.06.2003

(51)Int.Cl. G06F 17/60
G09C 1/00

(21)Application number : 2001-362788 (71)Applicant : JCB:KK

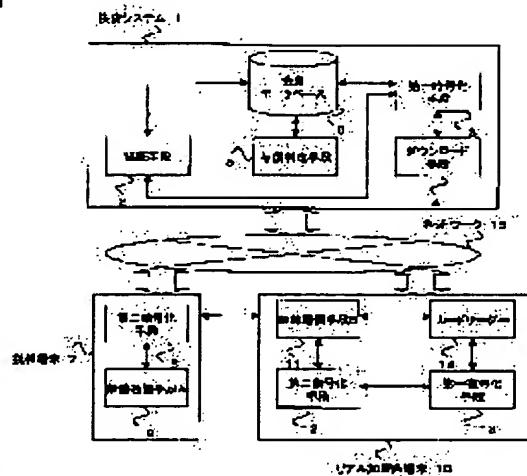
(22)Date of filing : 28.11.2001 (72)Inventor : SHIMOKAWA TAKAHIRO

(54) SETTLEMENT SYSTEM AND METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a settlement system and a method for making settlement by a card using a portable terminal of portable telephone or the like.

SOLUTION: In the settlement system, data can be transmitted/received between the portable terminal and a real member store terminal through a network, and the system includes a member database, a first encryption means that encrypts card information using a predetermined first cipher key to create first encryption data, a download means that transmits software and the first encryption data for making settlement by a card to the portable terminal, and a credit decision means that receives, from the real member store, a telegraphic message edited from a plaintext that has been converted from the encrypted card information directly received from the portable terminal by decrypting the information using a first decoding key corresponding to the first cipher key, and, based on the received telegraphic message, makes a credit decision of whether or not making settlement by the card of a user is to be approved based on the member database.



LEGAL STATUS

[Date of request for examination] 22.10.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-162680

(P2003-162680A)

(43) 公開日 平成15年6月6日(2003.6.6)

(51) Int.Cl. ⁷	識別記号	F I	テマコード(参考)
G 06 F 17/60	4 1 4	G 06 F 17/60	4 1 4 5 J 1 0 4
	2 4 2		2 4 2
	5 0 6		5 0 6
	5 1 2		5 1 2
	Z E C		Z E C

審査請求 未請求 請求項の数28 O L (全 18 頁) 最終頁に続く

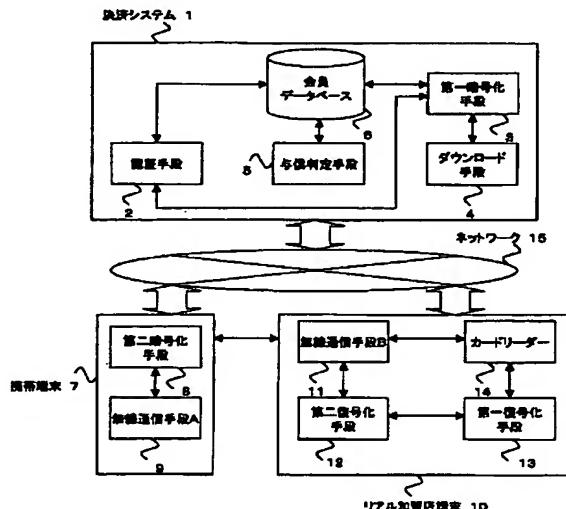
(21) 出願番号	特願2001-362788(P2001-362788)	(71) 出願人	593022629 株式会社ジェーシーピー 東京都千代田区神田駿河台1丁目6番地
(22) 出願日	平成13年11月28日(2001.11.28)	(72) 発明者	下川 卓宏 東京都千代田区神田駿河台一丁目6番地 株式会社ジェーシーピー情報ネットワーク 部内
		(74) 代理人	100100402 弁理士 名越 秀夫 (外1名) Fターム(参考) 5J104 NA02 NA35 PA07 PA10

(54) 【発明の名称】 決済システム及び方法

(57) 【要約】

【課題】携帯電話等の携帯端末を用いてカード決済を行う際の決済システム及び方法を提供することを目的とする。

【解決手段】決済システムに於いて、携帯端末とリアル加盟店端末との間でネットワークを介してデータの送受信が可能であって、会員データベースと、カード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成する第一暗号化手段と、カード決済を行わせる為のソフトウェア及び一次暗号化データを携帯端末に送信するダウンロード手段と、携帯端末から直接受信した暗号化されたカード情報を第一暗号キーに対応する第一復号化手段を用いて復号化して平文に変換し、平文から編集された電文をリアル加盟店端末から受信し、受信した電文に基づいてユーザのカード決済を承認するか否かの与信判定を、会員データベースに基づいて行う与信判定手段とを有する決済システムである。



【特許請求の範囲】

【請求項1】カード支払を行うユーザが有する携帯端末を介してカード決済を行う為の決済システムに於いて、前記携帯端末と、前記ユーザが商品等の購入を行うリアル店舗が有するリアル加盟店端末との間でネットワークを介してデータの送受信が可能であって、前記ユーザの情報及び／又は前記ユーザに関する情報及びカード情報を格納している会員データベースと、前記ユーザの前記カード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成する第一暗号化手段と、前記携帯端末と前記リアル加盟店端末との間で直接データの送受信を行いカード決済を行わせる為のソフトウェア及び前記一次暗号化データを前記携帯端末に送信するダウンロード手段と、前記リアル加盟店端末に於いて前記携帯端末から直接受信した暗号化されたカード情報を前記第一暗号キーに対応する第一復号キーを用いて復号化して平文に変換し、前記平文から編集された電文を前記リアル加盟店端末から受信し、前記受信した電文に基づいて前記ユーザのカード決済を承認するか否かの与信判定を、前記会員データベースに基づいて行う与信判定手段とを有することを特徴とする決済システム。

【請求項2】前記携帯端末は、前記決済システムから受信した前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成し、前記二次暗号化データを前記リアル加盟店端末に直接送信することを特徴とする請求項1に記載の決済システム。

【請求項3】前記リアル加盟店端末は、前記携帯端末から前記二次暗号化データを直接受信し、前記第二暗号キーに対応する第二復号キーを用いて前記一次暗号化データに復号後、更に第一復号キーを用いて復号化することを特徴とする請求項1又は請求項2に記載の決済システム。

【請求項4】カード支払を行うユーザが有する携帯端末を介してカード決済を行う為の決済システムに於いて、前記ユーザが商品等の購入を行うリアル店舗が有するリアル加盟店端末と、前記ユーザのカード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記リアル加盟店端末と前記ユーザが有する携帯端末との間で直接データの送受信を行う為のソフトウェアを送信する決済システムとの間でネットワークを介してデータの送受信が可能であって、前記携帯端末は、前記一次暗号化データを前記決済システムから受信し、前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成する第二暗号化手段と、前記二次暗号化データを前記リアル加盟店端末に直接送信する無線通信手段Aとを有することを特徴とする携帯端末。

【請求項5】カード支払を行うユーザが有する携帯端末を介してカード決済を行う為の決済システムに於いて、前記ユーザのカード情報を予め定められた第一暗号キー

を用いて暗号化し一次暗号化データを作成し、前記リアル加盟店端末と前記ユーザが有する携帯端末との間で直接データの送受信を行う為のソフトウェアを送信する決済システムと、前記携帯端末との間でネットワークを介してデータの送受信が可能であって、前記リアル加盟店端末は、前記携帯端末から暗号化されたカード情報を直接受信する無線通信手段Bと、前記第一暗号キーに対応する第一復号キーを用いて前記受信したカード情報を復号化して平文に変換する第一復号化手段と、前記第一復号化手段に於いて変換した平文を電文に変換し前記決済システムに送信するカードリーダーとを有することを特徴とするリアル加盟店端末。

【請求項6】前記携帯端末が前記決済システムから受信した前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成し、前記二次暗号化データを前記リアル加盟店端末に直接送信する場合には、前記リアル加盟店端末は、前記携帯端末から前記二次暗号化データを直接受信し、前記第二暗号キーに対応する第二復号キーを用いて前記一次暗号化データに復号する第二復号化手段を更に有し、前記第二復号化手段に於いて前記一次暗号化データに復号後、前記第一復号キーを用いて平文化することを特徴とする請求項5に記載のリアル加盟店端末。

【請求項7】前記リアル加盟店端末と前記携帯端末との間のデータの送受信は、ブルートゥース、赤外線通信のいずれかを含む無線通信を介して行うことと特徴とする請求項1から請求項6のいずれかに記載の決済システム。

【請求項8】ネットワークを介してカード決済を行う為の決済システムに於いて、前記カード支払を行うユーザが有するユーザ端末と、前記ユーザが商品等の購入を行うバーチャル加盟店端末との間でネットワークを介してデータの送受信が可能であって、前記ユーザの情報及び／又は前記ユーザに関する情報及びカード情報を格納している会員データベースと、前記ユーザの前記カード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成する第一暗号化手段と、前記第一暗号化手段に於いて作成した一次暗号化データを前記ユーザ端末に送信するダウンロード手段と、前記バーチャル加盟店端末に於いて前記ユーザ端末から受信した暗号化されたカード情報を前記第一暗号キーに対応する第一復号キーを用いて復号化して平文に変換し、前記平文から編集された電文を前記バーチャル加盟店端末から受信し、前記受信した電文に基づいて前記ユーザのカード決済を承認するか否かの与信判定を、前記会員データベースに基づいて行う与信判定手段とを有することを特徴とする決済システム。

【請求項9】前記ユーザ端末は、前記決済システムから受信した前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成し、前記二次暗

号化データを前記ネットワークを介して送信することを特徴とする請求項8に記載の決済システム。

【請求項10】前記バーチャル加盟店端末は、前記ユーザ端末から前記二次暗号化データを前記ネットワークを介して受信し、前記第二暗号キーに対応する第二復号キーを用いて前記一次暗号化データに復号後、更に第一復号キーを用いて復号化することを特徴とする請求項8又は請求項9に記載の決済システム。

【請求項11】ネットワークを介してカード決済を行う為の決済システムに於いて、カード支払を行うユーザが商品等の購入を行うバーチャル加盟店端末と、前記ユーザのカード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記作成した一次暗号化データを前記ユーザ端末に送信する決済システムとの間でネットワークを介してデータの送受信が可能であって、前記ユーザ端末は、前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成する第二暗号手段を有することを特徴とするユーザ端末。

【請求項12】ネットワークを介してカード決済を行う為の決済システムに於いて、カード支払を行うユーザのカード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記作成した一次暗号化データを前記ユーザ端末に送信する決済システムと、前記ユーザ端末との間でネットワークを介してデータの送受信が可能であって、前記バーチャル加盟店端末は、前記ユーザ端末から暗号化されたカード情報を前記ネットワークを介して受信し、前記第一暗号キーに対応する第一復号キーを用いて前記受信したカード情報を復号化して平文に変換する第一復号化手段と、前記第一復号化手段に於いて変換した平文を電文に変換し前記決済システムに送信するカード情報処理手段とを有することを特徴とするバーチャル加盟店端末。

【請求項13】前記ユーザ端末が前記決済システムから受信した前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成し、前記二次暗号化データを前記バーチャル加盟店端末に送信する場合には、前記バーチャル加盟店端末は、前記ユーザ端末から前記二次暗号化データを前記ネットワークを介して受信し、前記第二暗号キーに対応する第二復号キーを用いて前記一次暗号化データに復号する第二復号化手段を更に有し、前記第二復号化手段に於いて前記一次暗号化データに復号後、前記第一復号キーを用いて平文化することを特徴とする請求項12に記載のバーチャル加盟店端末。

【請求項14】前記第一復号キーは、予め前記決済システム及び／又は前記決済システムを有するカード会社から配布又は送信されていることを特徴とする請求項1から請求項13のいずれかに記載の決済システム。

【請求項15】カード支払を行うユーザが有する携帯端末を介してカード決済を行う為の決済方法に於いて、前記携帯端末と、前記ユーザが商品等の購入を行うリアル店舗が有するリアル加盟店端末との間でネットワークを介してデータの送受信が可能であって、前記ユーザの情報及び／又は前記ユーザに関する情報及びカード情報を会員データベースに格納しており、前記ユーザの前記カード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記携帯端末と前記リアル加盟店端末との間で直接データの送受信を行いカード決済を行わせる為のソフトウェア及び前記一次暗号化データを前記携帯端末に送信し、前記リアル加盟店端末に於いて前記携帯端末から直接受信した暗号化されたカード情報を前記第一暗号キーに対応する第一復号キーを用いて復号化して平文に変換し、前記平文から編集された電文を前記リアル加盟店端末から受信し、前記受信した電文に基づいて前記ユーザのカード決済を承認するか否かの与信判定を、前記会員データベースに基づいて行うことを特徴とする決済方法。

【請求項16】前記携帯端末は、前記決済システムから受信した前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成し、前記二次暗号化データを前記リアル加盟店端末に直接送信することを特徴とする請求項15に記載の決済方法。

【請求項17】前記リアル加盟店端末は、前記携帯端末から前記二次暗号化データを直接受信し、前記第二暗号キーに対応する第二復号キーを用いて前記一次暗号化データに復号後、更に第一復号キーを用いて復号化することを特徴とする請求項15又は請求項16に記載の決済方法。

【請求項18】カード支払を行うユーザが有する携帯端末を介してカード決済を行う為の決済方法に於いて、前記ユーザが商品等の購入を行うリアル店舗が有するリアル加盟店端末と、前記ユーザのカード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記リアル加盟店端末と前記ユーザが有する携帯端末との間で直接データの送受信を行う為のソフトウェアを送信する決済システムとの間でネットワークを介してデータの送受信が可能であって、前記携帯端末は、前記一次暗号化データを前記決済システムから受信し、前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成し、前記二次暗号化データを前記リアル加盟店端末に直接送信することを特徴とする携帯端末。

【請求項19】カード支払を行うユーザが有する携帯端末を介してカード決済を行う為の決済方法に於いて、前記ユーザのカード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記リアル加盟店端末と前記ユーザが有する携帯端末との間で直接データの送受信を行う為のソフトウェアを送信する決済

システムと、前記携帯端末との間でネットワークを介してデータの送受信が可能であって、前記リアル加盟店端末は、前記携帯端末から暗号化されたカード情報を直接受信する無線通信手段Bと、前記第一暗号キーに対応する第一復号キーを用いて前記受信したカード情報を復号化して平文に変換し、前記第一復号化手段に於いて変換した平文を電文に変換し送信することを特徴とするリアル加盟店端末。

【請求項20】前記携帯端末が前記決済システムから受信した前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成し、前記二次暗号化データを前記リアル加盟店端末に直接送信する場合には、前記リアル加盟店端末は、前記携帯端末から前記二次暗号化データを直接受信し、前記第二暗号キーに対応する第二復号キーを用いて前記一次暗号化データに復号し、前記一次暗号化データに復号後、前記第一復号キーを用いて平文化することを特徴とする請求項19に記載のリアル加盟店端末。

【請求項21】前記リアル加盟店端末と前記携帯端末との間のデータの送受信は、ブルートゥース、赤外線通信のいずれかを含む無線通信を介して行うことを特徴とする請求項15から請求項20のいずれかに記載の決済方法。

【請求項22】ネットワークを介してカード決済を行う為の決済方法に於いて、カード支払を行うユーザが有するユーザ端末と、前記ユーザが商品等の購入を行うバーチャル加盟店端末との間でネットワークを介してデータの送受信が可能であって、前記ユーザの情報及び／又は前記ユーザに関する情報及びカード情報を会員データベースに格納しており、前記ユーザの前記カード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記第一暗号化手段に於いて作成した一次暗号化データを前記ユーザ端末に送信し、前記バーチャル加盟店端末に於いて前記ユーザ端末から受信した暗号化されたカード情報を前記第一暗号キーに対応する第一復号キーを用いて復号化して平文に変換し、前記平文から編集された電文を前記バーチャル加盟店端末から受信し、前記受信した電文に基づいて前記ユーザのカード決済を承認するか否かの与信判定を、前記会員データベースに基づいて行うことを特徴とする決済方法。

【請求項23】前記ユーザ端末は、前記決済システムから受信した前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成し、前記二次暗号化データを前記ネットワークを介して送信することを特徴とする請求項22に記載の決済方法。

【請求項24】前記バーチャル加盟店端末は、前記ユーザ端末から前記二次暗号化データを前記ネットワークを介して受信し、前記第二暗号キーに対応する第二復号キーを用いて前記一次暗号化データに復号後、更に第一復号キーを用いて復号化することを特徴とする請求項22

又は請求項23に記載の決済方法。

【請求項25】ネットワークを介してカード決済を行う為の決済方法に於いて、カード支払を行うユーザが商品等の購入を行うバーチャル加盟店端末と、前記ユーザのカード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記作成した一次暗号化データを前記ユーザ端末に送信する決済システムとの間でネットワークを介してデータの送受信が可能であって、前記ユーザ端末は、前記一次暗号化データを前記決済システムから受信し、前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成することを特徴とするユーザ端末。

【請求項26】ネットワークを介してカード決済を行う為の決済システムに於いて、カード支払を行うユーザのカード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記作成した一次暗号化データを前記ユーザ端末に送信する決済システムと、前記ユーザ端末との間でネットワークを介してデータの送受信が可能であって、前記バーチャル加盟店端末は、前記ユーザ端末から暗号化されたカード情報を前記ネットワークを介して受信し、前記第一暗号キーに対応する第一復号キーを用いて前記受信したカード情報を復号化して平文に変換し、前記変換した平文を電文に変換し送信することを特徴とするバーチャル加盟店端末。

【請求項27】前記ユーザ端末が前記受信した前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成し、前記二次暗号化データを前記バーチャル加盟店端末に送信する場合には、前記バーチャル加盟店端末は、前記ユーザ端末から前記二次暗号化データを前記ネットワークを介して受信し、前記第二暗号キーに対応する第二復号キーを用いて前記一次暗号化データに復号し、前記一次暗号化データに復号後、前記第一復号キーを用いて平文化することを特徴とする請求項26に記載のバーチャル加盟店端末。

【請求項28】前記第一復号キーは、予めカード会社から配布又は送信されていることを特徴とする請求項15から請求項27のいずれかに記載の決済方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、携帯電話、P H S等の携帯端末又はネットワークを介してカード決済を行う際の決済システム及び方法に関する。

【0002】

【従来の技術】従来、商品等の購入を行う際にはその決済手段として現金決済の他に、クレジットカード、デビットカード等（以下、カード等）を用いて決済を行う方法（以下、カード決済）が存在している。これは商品等の購入を行う際に、カード等を提示し署名、暗証番号等によって正当なるカード等の所有者であるかの判別後、決済を行う方法である。

【0003】更に近年の通信技術等の技術発達に伴い、自動販売機等の従来ではカード等による決済が行えなかった機器に於いても、携帯端末を用いることによってカード等による決済を行う方法が提案されている。

【0004】上記の方法の一例が特開2001-134684号に開示されている。この公開公報に開示されている発明は、自動販売機等の機器にカード決済を行う装置を取り付け、前記装置と携帯電話との間で無線通信を介してデータの送受信を行い、カード等による決済を実現するものである。

【0005】

【発明が解決しようとする課題】特開2001-134684号公開公報に開示されている発明を用いた場合では、携帯電話とカード決済を行う装置との間での無線通信のセキュリティ面に問題点が存在している。即ち、例えば公知の無線通信技術であるブルートゥース、無線LAN等の電波を用いた場合では、携帯電話から全周囲に（携帯電話を中心として同心円上に）情報が発信されるので、不必要的方向に対しても情報が発信されてしまうこととなる。従って、悪意を有する者がこの情報を傍受して悪用することも可能である。

【0006】更に電波以外の、例えば指向性がある赤外線通信（IRDA）等を用いた方法もあるが、この場合には不必要的方向に対して情報が発信される問題は解決できるが、同方向の延長線上に悪意を有する者が存在した場合には、同様にこの情報を傍受して悪用することも可能である。

【0007】更に携帯電話を忘れる、落とす等は日常生活に於いて起こりえることであるが、上記公開公報に開示されている発明を単に用いた場合では、携帯電話を取得した第三者がそれを悪用して決済を行うことも可能である。

【0008】

【課題を解決するための手段】カード決済に於いて重要なことはセキュリティ面にある。つまり携帯端末からカード決済を行う装置に対して情報を送信した場合に、その情報が第三者によって傍受され悪用される可能性、落とした携帯電話等でそれを用いて第三者に悪用される可能性等である。

【0009】本発明者は上記問題点に鑑み、このセキュリティ面を重視することによる、より有効性のあるカード決済を行う決済システム及び方法を発明した。

【0010】更に携帯端末／ユーザ端末を用いた場合、従来はカード決済を行う装置（以下、カードリーダー）とカード会社とのカード決済用の情報処理システムを変更する必要があったが、本発明を用いることによって、従来のカードリーダーに無線通信とデータ復号化のユニットを単に接続するのみで、カードリーダーとカード会社とのカード決済用の情報処理システムについては何らの変更を加える必要性がない。従って、カード決済用の

情報処理システムの変更の手間負担、コスト負担を回避することが可能となる。

【0011】請求項1の発明は、カード支払を行うユーザが有する携帯端末を介してカード決済を行う為の決済システムに於いて、前記携帯端末と、前記ユーザが商品等の購入を行うリアル店舗が有するリアル加盟店端末との間でネットワークを介してデータの送受信が可能であって、前記ユーザの情報及び／又は前記ユーザに関する情報及びカード情報を格納している会員データベースと、前記ユーザの前記カード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成する第一暗号化手段と、前記携帯端末と前記リアル加盟店端末との間で直接データの送受信を行いカード決済を行わせる為のソフトウェア及び前記一次暗号化データを前記携帯端末に送信するダウンロード手段と、前記リアル加盟店端末に於いて前記携帯端末から直接受信した暗号化されたカード情報を前記第一暗号キーに対応する第一復号キーを用いて復号化して平文に変換し、前記平文から編集された電文を前記リアル加盟店端末から受信し、前記受信した電文に基づいて前記ユーザのカード決済を承認するか否かの与信判定を、前記会員データベースに基づいて行う与信判定手段とを有する決済システムである。

【0012】請求項15の発明は、カード支払を行うユーザが有する携帯端末を介してカード決済を行う為の決済方法に於いて、前記携帯端末と、前記ユーザが商品等の購入を行うリアル店舗が有するリアル加盟店端末との間でネットワークを介してデータの送受信が可能であって、前記ユーザの情報及び／又は前記ユーザに関する情報及びカード情報を会員データベースに格納しており、前記ユーザの前記カード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記携帯端末と前記リアル加盟店端末との間で直接データの送受信を行いカード決済を行わせる為のソフトウェア及び前記一次暗号化データを前記携帯端末に送信し、前記リアル加盟店端末に於いて前記携帯端末から直接受信した暗号化されたカード情報を前記第一暗号キーに対応する第一復号キーを用いて復号化して平文に変換し、前記平文から編集された電文を前記リアル加盟店端末から受信し、前記受信した電文に基づいて前記ユーザのカード決済を承認するか否かの与信判定を、前記会員データベースに基づいて行う決済方法である。

【0013】請求項2の発明は、前記携帯端末は、前記決済システムから受信した前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成し、前記二次暗号化データを前記リアル加盟店端末に直接送信する決済システムである。

【0014】請求項16の発明は、前記携帯端末は、前記決済システムから受信した前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを

作成し、前記二次暗号化データを前記リアル加盟店端末に直接送信する決済方法である。

【0015】請求項3の発明は、前記リアル加盟店端末は、前記携帯端末から前記二次暗号化データを直接受信し、前記第二暗号キーに対応する第二復号キーを用いて前記一次暗号化データに復号後、更に第一復号キーを用いて復号化する決済システムである。

【0016】請求項17の発明は、前記リアル加盟店端末は、前記携帯端末から前記二次暗号化データを直接受信し、前記第二暗号キーに対応する第二復号キーを用いて前記一次暗号化データに復号後、更に第一復号キーを用いて復号化する決済方法である。

【0017】請求項1から請求項3及び請求項15から請求項17の発明によって、セキュリティ面が向上した携帯端末を用いたカード決済の決済システムが可能となる。又従来のカード決済システムをそのまま用いることが可能となるので、システム導入の際に発生するコストを安価に抑えることが可能となる。尚、本明細書に於いて編集とは、平文を単にそのまま電文にする、平文に所定の事項を追加して電文にする、平文を加工して同内容の電文にする、又前記同内容の電文に所定の事項を更に追加する等を意味している。

【0018】請求項4の発明は、カード支払を行うユーザが有する携帯端末を介してカード決済を行う為の決済システムに於いて、前記ユーザが商品等の購入を行うリアル店舗が有するリアル加盟店端末と、前記ユーザのカード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記リアル加盟店端末と前記ユーザが有する携帯端末との間で直接データの送受信を行う為のソフトウェアを送信する決済システムとの間でネットワークを介してデータの送受信が可能であって、前記携帯端末は、前記一次暗号化データを前記決済システムから受信し、前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成する第二暗号化手段と、前記二次暗号化データを前記リアル加盟店端末に直接送信する無線通信手段Aとを有する携帯端末である。

【0019】請求項18の発明は、カード支払を行うユーザが有する携帯端末を介してカード決済を行う為の決済方法に於いて、前記ユーザが商品等の購入を行うリアル店舗が有するリアル加盟店端末と、前記ユーザのカード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記リアル加盟店端末と前記ユーザが有する携帯端末との間で直接データの送受信を行う為のソフトウェアを送信する決済システムとの間でネットワークを介してデータの送受信が可能であって、前記携帯端末は、前記一次暗号化データを前記決済システムから受信し、前記一次暗号化データを更に第二暗号キーを用いて暗号化し二次暗号化データを作成し、前記二次暗号化データを前記リアル加盟店端末に直接送

信する携帯端末である。

【0020】請求項4及び請求項18の発明によって、決済システムから送信された一次暗号化データを更に暗号化してリアル加盟店端末に送信することが可能となり、これによって、無線通信が傍受されても2重の暗号化が施されている為、解読が困難となり、セキュリティ面の向上に繋がる。

【0021】請求項5の発明は、カード支払を行うユーザが有する携帯端末を介してカード決済を行う為の決済システムに於いて、前記ユーザのカード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記リアル加盟店端末と前記ユーザが有する携帯端末との間で直接データの送受信を行う為のソフトウェアを送信する決済システムと、前記携帯端末との間でネットワークを介してデータの送受信が可能であって、前記リアル加盟店端末は、前記携帯端末から暗号化されたカード情報を直接受信する無線通信手段Bと、前記第一暗号キーに対応する第一復号キーを用いて前記受信したカード情報を復号化して平文に変換する第一復号化手段と、前記第一復号化手段に於いて変換した平文を電文に変換し前記決済システムに送信するカードリーダーとを有するリアル加盟店端末である。

【0022】請求項6の発明は、前記携帯端末が前記決済システムから受信した前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成し、前記二次暗号化データを前記リアル加盟店端末に直接送信する場合には、前記リアル加盟店端末は、前記携帯端末から前記二次暗号化データを直接受信し、前記第二暗号キーに対応する第二復号キーを用いて前記一次暗号化データに復号する第二復号化手段を更に有し、前記第二復号化手段に於いて前記一次暗号化データに復号後、前記第一復号キーを用いて平文化するリアル加盟店端末である。

【0023】請求項19の発明は、カード支払を行うユーザが有する携帯端末を介してカード決済を行う為の決済方法に於いて、前記ユーザのカード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記リアル加盟店端末と前記ユーザが有する携帯端末との間で直接データの送受信を行う為のソフトウェアを送信する決済システムと、前記携帯端末との間でネットワークを介してデータの送受信が可能であって、前記リアル加盟店端末は、前記携帯端末から暗号化されたカード情報を直接受信する無線通信手段Bと、前記第一暗号キーに対応する第一復号キーを用いて前記受信したカード情報を復号化して平文に変換し、前記第一復号化手段に於いて変換した平文を電文に変換し送信するリアル加盟店端末である。

【0024】請求項20の発明は、前記携帯端末が前記決済システムから受信した前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作

成し、前記二次暗号化データを前記リアル加盟店端末に直接送信する場合には、前記リアル加盟店端末は、前記携帯端末から前記二次暗号化データを直接受信し、前記第二暗号キーに対応する第二復号キーを用いて前記一次暗号化データに復号し、前記一次暗号化データに復号後、前記第一復号キーを用いて平文化するリアル加盟店端末である。

【0025】請求項5と請求項6及び請求項19と請求項20の発明によって、携帯端末から受信した暗号化されたカード情報を復号化し、それを従来通りのカードリーダーで決済システムに送信する為、カード決済に大幅な変更を加える必要性がなく、本発明の決済システムを安価に導入することが可能となる。

【0026】請求項8の発明は、ネットワークを介してカード決済を行う為の決済システムに於いて、前記カード支払を行うユーザが有するユーザ端末と、前記ユーザが商品等の購入を行うバーチャル加盟店端末との間でネットワークを介してデータの送受信が可能であって、前記ユーザの情報及び／又は前記ユーザに関する情報及びカード情報を格納している会員データベースと、前記ユーザの前記カード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成する第一暗号化手段と、前記第一暗号化手段に於いて作成した一次暗号化データを前記ユーザ端末に送信するダウンロード手段と、前記バーチャル加盟店端末に於いて前記ユーザ端末から受信した暗号化されたカード情報を前記第一暗号キーに対応する第一復号キーを用いて復号化して平文に変換し、前記平文から編集された電文を前記バーチャル加盟店端末から受信し、前記受信した電文に基づいて前記ユーザのカード決済を承認するか否かの与信判定を、前記会員データベースに基づいて行う与信判定手段とを有する決済システムである。

【0027】請求項9の発明は、前記ユーザ端末は、前記決済システムから受信した前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成し、前記二次暗号化データを前記ネットワークを介して送信する決済システムである。

【0028】請求項10の発明は、前記バーチャル加盟店端末は、前記ユーザ端末から前記二次暗号化データを前記ネットワークを介して受信し、前記第二暗号キーに対応する第二復号キーを用いて前記一次暗号化データに復号後、更に第一復号キーを用いて復号化する決済システムである。

【0029】請求項22の発明は、ネットワークを介してカード決済を行う為の決済方法に於いて、カード支払を行うユーザが有するユーザ端末と、前記ユーザが商品等の購入を行うバーチャル加盟店端末との間でネットワークを介してデータの送受信が可能であって、前記ユーザの情報及び／又は前記ユーザに関する情報及びカード情報を会員データベースに格納しており、前記ユーザの

前記カード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記第一暗号化手段に於いて作成した一次暗号化データを前記ユーザ端末に送信し、前記バーチャル加盟店端末に於いて前記ユーザ端末から受信した暗号化されたカード情報を前記第一暗号キーに対応する第一復号キーを用いて復号化して平文に変換し、前記平文から編集された電文を前記バーチャル加盟店端末から受信し、前記受信した電文に基づいて前記ユーザのカード決済を承認するか否かの与信判定を、前記会員データベースに基づいて行う決済方法である。

【0030】請求項23の発明は、前記ユーザ端末は、前記決済システムから受信した前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成し、前記二次暗号化データを前記ネットワークを介して送信する決済方法である。

【0031】請求項24の発明は、前記バーチャル加盟店端末は、前記ユーザ端末から前記二次暗号化データを前記ネットワークを介して受信し、前記第二暗号キーに対応する第二復号キーを用いて前記一次暗号化データに復号後、更に第一復号キーを用いて復号化する決済方法である。

【0032】請求項8から請求項10及び請求項22から請求項24の発明によって、セキュリティ面が向上したネットワークを介したカード決済の決済システムが可能となる。又従来のカード決済システムをそのまま用いることが可能となるので、システム導入の際に発生するコストを安価に抑えることが可能となる。

【0033】請求項11の発明は、ネットワークを介してカード決済を行う為の決済システムに於いて、カード支払を行うユーザが商品等の購入を行うバーチャル加盟店端末と、前記ユーザのカード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記作成した一次暗号化データを前記ユーザ端末に送信する決済システムとの間でネットワークを介してデータの送受信が可能であって、前記ユーザ端末は、前記一次暗号化データを前記決済システムから受信し、前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成する第二暗号化手段を有するユーザ端末である。

【0034】請求項25の発明は、ネットワークを介してカード決済を行う為の決済方法に於いて、カード支払を行うユーザが商品等の購入を行うバーチャル加盟店端末と、前記ユーザのカード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記作成した一次暗号化データを前記ユーザ端末に送信する決済システムとの間でネットワークを介してデータの送受信が可能であって、前記ユーザ端末は、前記一次暗号化データを前記決済システムから受信し、前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次

暗号化データを作成するユーザ端末である。

【0035】請求項11及び請求項25の発明によって、決済システムから送信された一次暗号化データを更に暗号化してバーチャル加盟店端末に送信することが可能となり、これによって、ネットワーク上に於いてユーザ端末とバーチャル加盟店端末との通信が傍受されても2重の暗号化が施されている為、解読が困難となり、セキュリティ面の向上に繋がる。

【0036】請求項12の発明は、ネットワークを介してカード決済を行う為の決済システムに於いて、カード支払を行うユーザのカード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記作成した一次暗号化データを前記ユーザ端末に送信する決済システムと、前記ユーザ端末との間でネットワークを介してデータの送受信が可能であって、前記バーチャル加盟店端末は、前記ユーザ端末から暗号化されたカード情報を前記ネットワークを介して受信し、前記第一暗号キーに対応する第一復号キーを用いて前記受信したカード情報を復号化して平文に変換する第一復号化手段と、前記第一復号化手段に於いて変換した平文を電文に変換し前記決済システムに送信するカード情報処理手段とを有するバーチャル加盟店端末である。

【0037】請求項13の発明は、前記ユーザ端末が前記決済システムから受信した前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成し、前記二次暗号化データを前記バーチャル加盟店端末に送信する場合には、前記バーチャル加盟店端末は、前記ユーザ端末から前記二次暗号化データを前記ネットワークを介して受信し、前記第二暗号キーに対応する第二復号キーを用いて前記一次暗号化データに復号する第二復号化手段を更に有し、前記第二復号化手段に於いて前記一次暗号化データに復号後、前記第一復号キーを用いて平文化するバーチャル加盟店端末である。

【0038】請求項26の発明は、ネットワークを介してカード決済を行う為の決済システムに於いて、カード支払を行うユーザのカード情報を予め定められた第一暗号キーを用いて暗号化し一次暗号化データを作成し、前記作成した一次暗号化データを前記ユーザ端末に送信する決済システムと、前記ユーザ端末との間でネットワークを介してデータの送受信が可能であって、前記バーチャル加盟店端末は、前記ユーザ端末から暗号化されたカード情報を前記ネットワークを介して受信し、前記第一暗号キーに対応する第一復号キーを用いて前記受信したカード情報を復号化して平文に変換し、前記変換した平文を電文に変換し送信するバーチャル加盟店端末である。

【0039】請求項27の発明は、前記ユーザ端末が前記受信した前記一次暗号化データを、更に第二暗号キーを用いて暗号化し二次暗号化データを作成し、前記二次暗号化データを前記バーチャル加盟店端末に送信する場

合には、前記バーチャル加盟店端末は、前記ユーザ端末から前記二次暗号化データを前記ネットワークを介して受信し、前記第二暗号キーに対応する第二復号キーを用いて前記一次暗号化データに復号し、前記一次暗号化データに復号後、前記第一復号キーを用いて平文化するバーチャル加盟店端末である。

【0040】請求項12と請求項13及び請求項26と請求項27の発明によって、ユーザ端末から受信した暗号化されたカード情報を復号化し、それを従来通りのカード情報処理手段で決済システムに送信する為、カード決済に大幅な変更を加える必要性がなく、本発明の決済システムを安価に導入することが可能となる。

【0041】請求項14の発明は、前記第一復号キーは、予め前記決済システム及び／又は前記決済システムを有するカード会社から配布又は送信されている決済システムである。

【0042】請求項28の発明は、前記第一復号キーは、予めカード会社から配布又は送信されている決済方法である。

【0043】

【発明の実施の形態】本発明の実施態様の一例を図を用いて詳細に説明する。図1及び図2は本発明の決済システム1のシステム構成の一例である。図1は、実在する店舗（以下、リアル加盟店とする）に於いてユーザ（カード等を用いた決済を行う者）が当該店舗に赴きカード決済を行う場合を示し、図2は、オンラインショッピング等のネットワーク15上に存在する店舗（以下、バーチャル加盟店とする）に於いてユーザがネットワーク15を介してカード決済を行う場合のシステム構成を示した図である。

【0044】まず図1に於けるユーザがリアル加盟店で決済システム1を用いる場合を説明する。決済システム1は、ユーザが有する携帯端末7とリアル加盟店が有するリアル加盟店端末10と決済システム1とがネットワーク15を介してデータの送受信が可能である。又携帯端末7の無線通信手段A9とリアル加盟店端末10の無線通信手段B11とは、ブルートゥース、IrDA等の無線通信を行う手段であって、直接データの送受信が可能である。

【0045】決済システム1は、カード決済を行うカード会社等が有するシステムであって、認証手段2と第一暗号化手段3とダウンロード手段4と与信判定手段5と会員データベース6とを有している。

【0046】認証手段2は、携帯端末7からアクセス要求を受信した際に正当なるユーザであるか否かの認証を行う手段である。この認証の際には、ユーザ本人を認証する為の認証情報（IDやパスワード等）、電話番号、住所等を用いて行う。

【0047】第一暗号化手段3は、ユーザが有する携帯端末7に対してカード情報（ユーザのカード番号とカ

ト有効期限)を予め定められた暗号化方法によって、第一暗号キーで暗号化する手段である。この暗号化方法には公知のDES等を用いた共通鍵暗号方式、RSA等を用いた公開鍵暗号方式が該当する。即ちユーザがカード決済に用いるカード情報(例えば、「3540123456789」「01/05」最初の括弧がカード番号、最後の括弧が有効期限を示している)を予め定められた第一暗号キーで暗号化し、一次暗号化データ(例えば、「*%\$#=+%\$&@+}{-+-/○×」)を作成する。

【0048】ダウンロード手段4は、携帯端末7とリアル加盟店端末10との間で直接データの送受信を行いカード決済を行わせる為のソフトウェアを、携帯端末7に送信する手段である。尚、セキュリティ性を向上させる為に、第一暗号化手段3で暗号化された一次暗号化データを更にワンタイムパスワード等を用いることによって携帯端末7で暗号化させる為のプログラム(第二暗号化手段8)を、当該ソフトウェアに組み込んでも良い。

【0049】与信判定手段5は、リアル加盟店端末10からネットワーク15を介して送信されたカード情報を受信し、当該カード決済の対象となるユーザの限度額等を会員データベース6を参照し、ユーザのカード決済を承認するか否かの与信判定を行う手段である。つまり従来のカード決済に於ける与信判定と同等の処理を行う手段である。

【0050】会員データベース6は、決済システム1を利用するユーザの情報を格納しているデータベースである。ユーザの情報の一例としては、本人を認証する情報(IDやパスワード)、ユーザに関する情報(氏名、住所、電話番号等)、カード情報(カード番号、カード有効期限)等を格納しているデータベースである。

【0051】携帯端末7は、ネットワーク15機能を有する携帯電話、PHS、PDA、ノート型パソコン等であるがこれに限定されず、通常のパーソナルコンピュータであっても良い。

【0052】携帯端末7は、第二暗号化手段8と無線通信手段A9とを有する。

【0053】第二暗号化手段8は、決済システム1のダウンロード手段4から受信したソフトウェアに組み込まれている、第一暗号化手段3で暗号化された一次暗号化データを更にワンタイムパスワード等の第二暗号キーを用いることによって更に暗号化し、二次暗号化データを作成する為のプログラムである。ここでワンタイムパスワードとして、一次暗号化データを、第二暗号化手段8に於いて暗号化する時刻等を第二暗号キーとして用いることによって暗号化する方法をその一例とするが、それ以外であっても良い。

【0054】例えば、一次暗号化データを暗号化する時刻を第二暗号キーとしており、その時刻が14時33分であった場合には、第二暗号キーが「1433」とな

り、一次暗号化データが「*%\$#=+%\$&@+}{-+-/○×」であった場合、これを第二暗号化手段8に於いて「xyz\$0q1!#@*<N?&#!p」と二次暗号化データを作成する。

【0055】無線通信手段A9は、リアル加盟店端末10が有する無線通信手段B11と直接データの送受信が可能なデータ送受信手段であって、ブルートゥース、IrDA等の公知の無線通信手段を示す。上記例の場合では、二次暗号化データ「xyz\$0q1!#@*<N?&#!p」を送信する。

【0056】リアル加盟店端末10は、リアル店舗が有しているカード決済をカード会社との間でデータ処理する為のシステムであって、無線通信手段B11と第二復号化手段12と第一復号化手段13とカードリーダー14とを有している。

【0057】無線通信手段B11は、携帯端末7が有する無線通信手段A9と直接データの送受信が可能なデータ送受信手段であって、ブルートゥース、IrDA等の公知の無線通信手段を示す。上記例の場合では、二次暗号化データ「xyz\$0q1!#@*<N?&#!p」を受信する。

【0058】第二復号化手段12は、携帯端末7の第二暗号化手段8に於いて暗号化され、無線通信手段B11が携帯端末7から受信した二次暗号化データを、第二復号キーを用いて復号化する為の手段である。第二復号キーは、第二暗号キーを復号する為の復号キーを意味し、例えば第二暗号キーが時刻の場合には、第二復号キーも時刻となる。第二暗号化手段8に於いて暗号化する時刻が第二暗号キーの場合には、当該時刻が第二復号キーとなる。つまり、第二暗号化手段8に於いて一次暗号データを暗号化し、二次暗号化データを作成する時刻と、無線通信手段A9及び無線通信手段B11を介してリアル加盟店端末10に於いて二次暗号化データを携帯端末7から受信し、第二復号化手段12に於いて復号する際の時刻とは、ほぼ同一であるので当該時刻を用いても正常に暗号化/復号化が可能となる。

【0059】例えば上記例の場合では、無線通信手段B11が受信した二次暗号化データ「xyz\$0q1!#@*<N?&#!p」を第二復号キー「1433」で一次暗号化データ「*%\$#=+%\$&@+}{-+-/○×」に復号化する。

【0060】第一復号化手段13は、第二復号化手段12に於いて二次暗号化データが復号され、一次暗号データとなったデータを、更に第一復号キーを用いて復号化する為の手段である。第一復号キーは、第一暗号キーを復号する為の復号キーを意味し、決済システム1の第一暗号化手段3で暗号化された一次暗号データを復号化するものである。つまり、一次暗号データを復号化することによって、ユーザのカード決済に用いるカード情報を平文化することが可能となる。又第一暗号キーは、予め

決済システム1（又はカード会社）からCD-ROM等の電子記録媒体を用いて配布又はデータとして送信されており、場合によっては予めチップ等に書き込まれていても良い。

【0061】上記例の場合では、第二復号化手段12に於いて復号化した一次暗号化データ「*%\$#=+%\$&@+」{+-／○×}を、予め定められている第一復号キーで復号化することによって、カード情報を「3540123456789」に平文化することなる。

【0062】カードリーダー14は、従来のカード決済を行う際の磁気式クレジットカード等を読み取る為のカードリーダー14と同等の機能を有する処理システムであり、ネットワーク15を介してカード会社が有する決済システム1との間で第一復号化手段13によって平文化されたカード情報の送受信を行い、カード決済を行う手段である。

【0063】次に図2に於けるユーザがバーチャル加盟店で決済システム1を用いる場合を説明する。尚図1のシステム構成と同一部分については簡略化の為、説明を省略する。決済システム1は、ユーザが有するユーザ端末18とバーチャル加盟店が有するバーチャル加盟店端末17と決済システム1とがネットワーク15を介してデータの送受信が可能である。

【0064】決済システム1の認証手段2は、ユーザ端末18からアクセス要求を受信した際に正当なるユーザであるか否かの認証を行う手段である。

【0065】第一暗号化手段3は、ユーザが有するユーザ端末18に対してカード情報（ユーザのカード番号とカード有効期限）を予め定められた暗号化方法によって、第一暗号キーで暗号化する手段である。暗号化する方法等は、図1と同様である。

【0066】ダウンロード手段4は、ユーザ端末18とバーチャル加盟店端末17との間で直接データの送受信を行いカード決済を行わせる為のソフトウェアを、ユーザ端末18に送信する手段である。

【0067】与信判定手段5は、バーチャル加盟店端末17からネットワーク15を介して送信されたカード情報を受信し、当該カード決済の対象となるユーザの限度額等を会員データベース6を参照し、ユーザのカード決済を承認するか否かの与信判定を行う手段である。

【0068】会員データベース6は、決済システム1を利用するユーザの情報を格納しているデータベースである。

【0069】ユーザ端末18は、ネットワーク15機能を有する携帯電話、PHS、PDA、パソコンコンピュータを示す。

【0070】ユーザ端末18は、第二暗号化手段8を有する。

【0071】第二暗号化手段8は、決済システム1のダ

ウンロード手段4から受信したソフトウェアに組み込まれている、第一暗号化手段3で暗号化された一次暗号化データを更にワンタイムパスワード、SSLで用いる暗号キー等の第二暗号キーを用いることによって更に暗号化し、二次暗号化データを作成する為のプログラムである。第二暗号キー等は図1と同様である。

【0072】バーチャル加盟店端末17は、バーチャル店舗に於けるカード決済をカード会社との間でデータ処理する為のシステムであって、第二復号化手段12と第一復号化手段13とカード情報処理手段16とを有している。バーチャル加盟店端末17は、バーチャル店舗が有していても良いし、それ以外の他の者が有していても良い。

【0073】第二復号化手段12は、ユーザ端末18の第二暗号化手段8に於いて暗号化され、ネットワーク15を介してユーザ端末18から受信した二次暗号化データを、第二復号キーを用いて復号化する為の手段である。第二復号キー等は、図1と同様である。

【0074】第一復号化手段13は、第二復号化手段12に於いて二次暗号化データが復号され、一次暗号データとなったデータを、更に第一復号キーを用いて復号化する為の手段である。第一復号キー等は、図1と同様である。

【0075】カード情報処理手段16は、従来のカード決済を行う際と同等の機能を有する処理システムであり、ネットワーク15を介してカード会社が有する決済システム1との間で第一復号化手段13によって平文化されたカード情報の送受信を行い、カード決済を行う手段である。

【0076】

【実施例】次に本発明のプロセスの流れの一例を図3及び図4のフローチャート図と図1及び図2のシステム構成図とを用いて詳細に説明する。図3及び図4は、携帯端末7又はユーザ端末18と、リアル加盟店端末10又はバーチャル加盟店端末17との間で直接データの送受信を行いカード決済を行わせる（第二暗号化手段8を含む）為のソフトウェアを、携帯端末7又はユーザ端末18に送信する（ダウンロードさせる）場合のフローチャート図である。

【0077】まず図3に示した、ソフトウェアを携帯端末7又はユーザ端末18に送信する際のプロセスの流れの一例を示す。本プロセスは、予めユーザのカード情報を第一暗号化手段3に於いて一次暗号化データとし、当該一次暗号化データをインプリメントしたソフトウェアを携帯端末7又はユーザ端末18に送信する場合である。

【0078】ユーザは自らが有する携帯端末7又はユーザ端末18からネットワーク15を介して決済システム1にアクセスする（S100）。S100に於いて携帯端末7又はユーザ端末18と決済システム1との間で接

続が確立後、ユーザは携帯端末7又はユーザ端末18から決済システム1の認証手段2に対してID、パスワード等の認証情報を送信する(S110)。

【0079】S110に於いて送信された認証情報を受信した認証手段2は、前記認証情報を、会員データベース6に格納している認証情報に基づいて認証を行い、正規のユーザであるか否かの認証を行う(S120)。

【0080】S120の認証の結果、認証が出来なかつた場合には認証手段2は携帯端末7又はユーザ端末18に対してエラーメッセージを送信する(S130)。S120に於いて認証が行えた場合には、第一暗号化手段3が、当該認証を行ったユーザの会員データベース6に格納しているカード情報を予め定められている第一暗号キーで暗号化し、一次暗号化データを作成する(S140)。

【0081】例えばカード情報が「3540123456789」「01/05」であった場合、予め定められた第一暗号キーで暗号化し、一次暗号化データ(例えば、「*%\$#=&%\$&#@+}{-+-/○×」)を作成する。

【0082】S140に於いて作成した一次暗号化データを、前記ソフトウェアにインプリメントしてダウンロード手段4が、当該ソフトウェアを携帯端末7又はユーザ端末18に送信し、ダウンロードさせる(S150)。

【0083】S150に於いてネットワーク15を介して携帯端末7又はユーザ端末18に送信したソフトウェアを携帯端末7又はユーザ端末18が格納することによって、図3のプロセスを終了する。

【0084】次に図4に示した、ソフトウェアを携帯端末7又はユーザ端末18に送信する際のプロセスの流れの一例を示す。本プロセスは、ユーザのカード情報を除いた部分(携帯端末7又はユーザ端末18とリアル加盟店端末10又はバーチャル加盟店端末17との間で直接データの送受信を行いカード決済を行わせる(第二暗号化手段8を含む)部分)のみのソフトウェアをまず送信し、その後ユーザからの要求に伴って、ユーザのカード情報を第一暗号化手段3に於いて暗号化することにより一次暗号化データを作成し、当該一次暗号化データをダウンロードが別途携帯端末7又はユーザ端末18に送信し、携帯端末7又はユーザ端末18に於いて当該ソフトウェアに一次暗号化データを組み込む方法である。従ってソフトウェアと一次暗号化データのダウンロードは同時に実行しても良い。

【0085】ユーザは自らが有する携帯端末7又はユーザ端末18からネットワーク15を介して決済システム1にアクセスする(S200)。S200に於いて携帯端末7又はユーザ端末18と決済システム1との接続が確立後、ユーザは携帯端末7又はユーザ端末18からダウンロード手段4に対して、ユーザのカード情報を除い

た部分(携帯端末7又はユーザ端末18とリアル加盟店端末10又はバーチャル加盟店端末17との間で直接データの送受信を行いカード決済を行わせる(第二暗号化手段8を含む)部分)のみのソフトウェアのダウンロードの要求を送信する(S210)。

【0086】S210に於けるダウンロードの要求を受信後、ダウンロード手段4は、ユーザのカード情報を除いた部分のみのソフトウェアを携帯端末7又はユーザ端末18に送信し、ダウンロードを行わせる(S220)。

【0087】S220に於いて送信されたカード情報を除いた部分のみのソフトウェアを携帯端末7又はユーザ端末18に於いて受信、格納し、その後(同時でなくとも後であっても良い)携帯端末7又はユーザ端末18を用いたカード決済を行う前までに携帯端末7又はユーザ端末18から決済システム1に再度アクセスし、携帯端末7又はユーザ端末18から認証手段2に認証情報を送信し(S230)、正規のユーザであるか否かの認証を認証手段2に行わせる。認証の方法は図3の場合と同様で良い。

【0088】S230に於いて送信された認証情報を受信した認証手段2は、認証を行い正規のユーザであるか否かの認証を行う(S240)。

【0089】S240の認証の結果、認証できなかった場合には、認証手段2は携帯端末7又はユーザ端末18に対してエラーメッセージを送信する(S250)。S240に於いて認証できた場合には第一暗号化手段3が、当該認証を行ったユーザのカード情報を予め定められている第一暗号キーを用いて暗号化し一次暗号化データを作成する(S260)。

【0090】一次暗号化データを作成後、ダウンロード手段4がネットワーク15を介して一次暗号化データを携帯端末7又はユーザ端末18に送信する(S270)。S270に於いてネットワーク15を介して送信された一次暗号化データを携帯端末7又はユーザ端末18に於いて受信後、携帯端末7又はユーザ端末18が受信した一次暗号化データを、S220に於いて格納したソフトウェアに組み込み、携帯端末7又はユーザ端末18に於いて格納することによって図4のプロセスを終了する。

【0091】次に、図3又は図4のプロセスを経てソフトウェアをダウンロード後、当該ソフトウェアを用いてカード決済を行う際のプロセスの流れの一例を示す。まず図5及び図6に於いて、リアル加盟店に於ける場合を説明する。

【0092】リアル加盟店に於けるリアル加盟店端末10には、予め決済システム1又はカード会社からリアル加盟店端末10の第一復号化手段13に於ける第一復号キーが配布され組み込まれている。ここで第一復号キーとは、決済システム1の第一暗号化手段3に於いてカ

ド情報を一次暗号化データに暗号化する第一暗号キーに対応し、一次暗号化データを平文のカード情報に復号化する復号キーを示す。又第一復号キーのリアル加盟店端末10に対する配布は、リアル加盟店端末10のチップに予め記憶させておく、ネットワーク15を介して決済システム1からリアル加盟店端末10の第一区豪華手段に送信する、CD-ROM等の記録媒体による配布等がある。

【0093】ユーザがリアル加盟店端末10に於いて決済を行う場合には、当該ソフトウェアを格納した携帯端末7のソフトウェアの一覧から、当該カード決済用のソフトウェア（図3又は図4でダウンロードしたソフトウェア）を起動する（S300）。

【0094】ソフトウェア起動後、当該ソフトウェアを正当に使用できるユーザか否かの判定を行う為、パスワード等の認証情報を入力させる（S310）。認証を行う為の認証画面の一例を図9に示す。この際に、複数のカード会社のカード決済が行えるように、その種類の選択（カード会社の選択）を行わせても良い。

【0095】S310に於いて入力した認証情報が正当であるか否かの判定を行い（S320）、不当な入力であれば再度入力を促す。又正当なる入力であれば、カードの正当なる使用者であると見なして、購入意思確認画面を起動する。図10に購入意思確認画面の一例を示す。

【0096】ユーザの購入意思を確認後（購入意思確認画面の「送信」ボタンを押す等）、S150に於いてダウンロードしたソフトウェアに組み込まれた一次暗号化データ又はS270に於いて決済システム1から送信され携帯端末7に於いて受信した一次暗号化データを、携帯端末7の第二暗号化手段8に於いて第二暗号キーを用いて更に暗号化し二次暗号化データを作成する（S330）。

【0097】例えば一次暗号化データが「*%\$#= &%\$&@+ { -+- / @X 」であって、その一次暗号化データを第二暗号化手段8に於いて暗号化する時刻が14時33分であった場合（ワンタイムパスワード（第二暗号キー）として暗号化する時刻を用いている場合）には第二暗号キーが「1433」となり、その結果第二暗号化手段8に於いて一次暗号化データが更に「x y z y \$" 0 q 1 ! # @ * < N ? & ! p 」と暗号化されることとなる。

【0098】S330に於いて二次暗号化データを作成後、携帯端末7の無線通信手段A9を介して二次暗号化データをリアル加盟店端末10に対して直接送信する（S340）。

【0099】S340に於いて無線通信手段A9から送信された二次暗号化データを、リアル加盟店端末10の無線通信手段B11に於いて受信後、第二復号化手段12が二次暗号化データを第二復号キーを用いて復号化す

る（S350）。

【0100】上記例の場合、無線通信手段B11に於いて受信した二次暗号化データが「x y z y \$" 0 q 1 ! # @ * < N ? & ! p 」であって、その二次暗号化データを第二復号化手段12に於いて復号化する時刻が14時33分であるので、第二復号キーが「1433」となり、その結果第二復号化手段12に於いて二次暗号化データが「*%\$#= &%\$&@+ { -+- / @X 」と一次暗号化データに復号される。

10 【0101】第二復号化手段12に於いて一次暗号化データに復号後、第一復号化手段13に於いて、一次暗号化データを第一復号キーを用いて平文に復号化する（S360）。

【0102】上記例の場合、一次暗号化データが「*%\$#= &%\$&@+ { -+- / @X 」であるので、予め決済システム1又はカード会社から配布された第一復号キーを用いて復号化し、「3540123456789」「01/05」とカード情報を平文化することとなる。

20 【0103】第一復号化手段13に於いて復号後、平文化したカード情報をリアル加盟店端末10のカードリーダー14が、正規のカードデータとして復号されているか否かの精査を行い（S370）、精査の結果何らかの異常が発生している場合には、エラーメッセージを無線通信手段B11を介して携帯端末7に送信する（S380）。携帯端末7の無線通信手段A9は、無線通信手段B11から受信したエラーメッセージを表示し通知する。

30 【0104】S370の精査の結果異常がなければ、カードリーダー14が平文化されたカードデータに基づいて電文を編集して、決済システム1に電文を送信する（S390）。ここで電文とは従来の磁気式クレジットカードを用いたカード決済と同様に、カード情報を予め定められた形式に変換し、購入商品等のカード決済に対する付随情報と共にカード会社に於いて決済する際の公知のフォーマットに対応したデータをいい、従来のカード決済の際のカードリーダー14からカード会社に対して送信しているデータと同様のデータを示す。

40 【0105】リアル加盟店端末10からネットワーク15を介して送信された電文を受信した決済システム1の与信判定手段5は、会員データベース6を参照して当該ユーザに対してカード決済を行っても良いか否かの与信判定を会員データベース6に格納している限度額等の情報に基づいて行い（S400）、限度額超過等の理由から決済を認めない場合には、与信拒否報告を与信判定手段5がリアル加盟店端末10のカードリーダー14に送信する。

50 【0106】与信拒否報告を受信したカードリーダー14は、無線通信手段B11を介して携帯端末7に与信拒否報告を送信する（S410）。S410に於いて送信

された与信拒否報告を携帯端末7の無線通信手段A9で受信すると、携帯端末7上に於いて当該ソフトウェアが与信が拒否された旨の与信拒否画面を表示する(S420)。与信拒否画面の一例を図11に示す。

【0107】S400の判定の結果、当該ユーザに対して決済を認める場合には、与信許可報告を与信判定手段5がリアル加盟店端末10のカードリーダー14に送信する。与信許可報告を受信したカードリーダー14は、無線通信手段B11を介して携帯端末7に与信許可報告を送信する(S430)。S430に於いて送信された与信許可報告を携帯端末7の無線通信手段A9で受信すると、携帯端末7上に於いて当該ソフトウェアが与信が許可され、決済が終了した旨の完了画面を表示する(S440)。図12に完了画面の一例を示す。

【0108】このように、S300からS440の一連のプロセスを実行することによって、又リアル加盟店端末10では従来のカードリーダー14に加えて、単に無線通信手段B11と第一復号化手段13、第二復号化手段12を併設するのみで、従来よりもセキュリティ性が向上し、且つカードリーダー14からカード会社に於けるカード決済の仕組みには何らの変化も加えずにその処理が可能となる。

【0109】次に図7及び図8に於けるネットワーク15上のバーチャル店舗に於いて決済を行う場合のプロセスの流れの一例を図2のシステム構成図を用いて詳細に説明する。

【0110】バーチャル加盟店端末17には、予め決済システム1又はカード会社からバーチャル加盟店端末17の第一復号化手段13に於ける第一復号キーが配布され組み込まれている。ここで第一復号キーとは、決済システム1の第一暗号化手段3に於いてカード情報を一次暗号化データに暗号化する第一暗号キーに対応し、一次暗号化データを平文のカード情報を復号化する復号キーを示す。又第一復号キーのバーチャル加盟店端末17に対する配布は、バーチャル加盟店端末17のチップに予め記憶させておく、ネットワーク15を介して決済システム1からバーチャル加盟店端末17の第一区豪華手段に送信する、CD-ROM等の記録媒体による配布等がある。

【0111】ユーザがバーチャル加盟店端末17に於いて決済を行う場合には、当該ソフトウェアを格納したユーザ端末18のソフトウェアの一覧から、当該カード決済用のソフトウェア(図3又は図4でダウンロードしたソフトウェア)を起動する(S500)。

【0112】ソフトウェア起動後、当該ソフトウェアを正当に使用できるユーザか否かの判定を行う為、パスワード等の認証情報を入力させる(S510)。この際に、複数のカード会社のカード決済が行えるように、その種類の選択(カード会社の選択)を行わせてても良い。

【0113】S510に於いて入力した認証情報が正当

であるか否かの判定を行い(S520)、不当な入力であれば再度入力を促す。又正当なる入力であれば、カードの正当なる使用者であると見なして、購入意思確認画面を起動する。

【0114】ユーザの購入意思を確認後(購入意思確認画面の「送信」ボタンを押す等)、S150に於いてダウンロードしたソフトウェアに組み込まれた一次暗号化データ又はS270に於いて決済システム1から送信されユーザ端末18に於いて受信した一次暗号化データを、ユーザ端末18の第二暗号化手段8に於いて第二暗号キーを用いて更に暗号化し二次暗号化データを作成する(S530)。

【0115】例えば一次暗号化データが「*%\$#= &%\$&@+ { -+- / @X 》 { -+- / @X 》 である、その一次暗号化データを第二暗号化手段8に於いて暗号化する時刻が14時33分であった場合(ワンタイムパスワード(第二暗号キー)として暗号化する時刻を用いている場合)には第二暗号キーが「1433」となり、その結果第二暗号化手段8に於いて一次暗号化データが更に「x y z y \$ " 0 q 1 ! # @ * < N ? & ! p 」と暗号化されることとなる。

【0116】S530に於いて二次暗号化データを作成後、二次暗号化データをネットワーク15を介してバーチャル加盟店端末17に対して送信する(S540)。

【0117】S540に於いて送信された二次暗号化データを、バーチャル加盟店端末17に於いて受信後、第二復号化手段12が二次暗号化データを第二復号キーを用いて復号化する(S550)。

【0118】上記例の場合、受信した二次暗号化データが「x y z y \$ " 0 q 1 ! # @ * < N ? & ! p 」であって、その二次暗号化データを第二復号化手段12に於いて復号化する時刻が14時33分であるので、第二復号キーが「1433」となり、その結果第二復号化手段12に於いて二次暗号化データが「*%\$#= &%\$&@+ { -+- / @X 》 と一次暗号化データに復号される。

【0119】第二復号化手段12に於いて一次暗号化データに復号後、第一復号化手段13に於いて、一次暗号化データを第一復号キーを用いて平文に復号化する(S560)。

【0120】上記例の場合、一次暗号化データが「*%\$#= &%\$&@+ { -+- / @X 》 であるので、予め決済システム1又はカード会社から配布された第一復号キーを用いて復号化し、「3540123456789」「01/05」とカード情報を平文化することなる。

【0121】第一復号化手段13に於いて復号後、平文化したカード情報をバーチャル加盟店端末17のカード情報処理手段16が、正規のカードデータとして復号されているか否かの精査を行い(S570)、精査の結果

何らかの異常が発生している場合には、エラーメッセージをカード情報処理手段16がユーザ端末18に送信する(S580)。ユーザ端末18は、ネットワーク15を介して受信したエラーメッセージを表示し通知する。

【0122】S570の精査の結果異常がなければ、カードリーダー14が平文化されたカードデータに基づいて電文を編集して、決済システム1に電文を送信する(S590)。ここで電文とは従来のネットワーク15を介したカード決済と同様に、カード情報を予め定められた形式に変換し、購入商品等のカード決済に対する付随情報と共にカード会社に於いて決済する際の公知のフォーマットに対応したデータをいい、従来のカード決済の際にカード会社に対して送信しているデータと同様のデータを示す。

【0123】バーチャル加盟店端末17からネットワーク15を介して送信された電文を受信した決済システム1の与信判定手段5は、会員データベース6を参照して当該ユーザに対してカード決済を行っても良いか否かの与信判定を会員データベース6に格納している限度額等の情報に基づいて行い(S600)、限度額超過等の理由から決済を認めない場合には、与信拒否報告を与信判定手段5がバーチャル加盟店端末17のカード情報処理手段16に送信する。

【0124】与信拒否報告を受信したカード情報処理手段16は、ネットワーク15を介してユーザ端末18に与信拒否報告を送信する(S610)。S610に於いて送信された与信拒否報告をユーザ端末18で受信すると、ユーザ端末18上に於いて当該ソフトウェアが与信が拒否された旨の与信拒否画面を表示する(S620)。

【0125】S600の判定の結果、当該ユーザに対して決済を認める場合には、与信許可報告を与信判定手段5がバーチャル加盟店端末17のカード情報処理手段16に送信する。与信許可報告を受信したカード情報処理手段16は、ネットワーク15を介してユーザ端末18に与信許可報告を送信する(S630)。S630に於いて送信された与信許可報告をユーザ端末18で受信すると、ユーザ端末18上に於いて当該ソフトウェアが与信が許可され、決済が終了した旨の完了画面を表示する(S640)。

【0126】このように、S500からS640の一連のプロセスを実行することによって、又バーチャル加盟店端末17では従来のカード情報処理手段16に加えて、単に第一復号化手段13、第二復号化手段12を併設するのみで、従来よりもセキュリティ性が向上し、且つカード情報処理手段16からカード会社に於けるカード決済の仕組みには何らの変化も加えずにその処理が可能となる。

【0127】本発明に於ける各手段、データベースは、その機能が論理的に区別されているのみであって、物理

上あるいは事実上同一の領域を為していても良い。又データベースの代わりにデータファイルであっても良いことは言うまでもなく、データベースとの記載にはデータファイルをも含んでいる。

【0128】尚、本発明を実施するにあたり本実施態様の機能を実現するソフトウェアのプログラムを記録した記憶媒体をシステムに供給し、そのシステムのコンピュータが記憶媒体に格納されたプログラムを読み出し実行することによって実現されることは当然である。

10 【0129】この場合、記憶媒体から読み出されたプログラム自身が前記した実施態様の機能を実現することとなり、そのプログラムを記憶した記憶媒体は本発明を当然のことながら構成することになる。

【0130】プログラムを供給する為の記憶媒体としては、例えばフロッピー(登録商標)ディスク、ハードディスク、光ディスク、光磁気ディスク、磁気テープ、不揮発性のメモリカード等を使用することができます。

20 【0131】又、コンピュータが読み出したプログラムを実行することにより、上述した実施態様の機能が実現されるだけではなく、そのプログラムの指示に基づき、コンピュータ上で稼働しているオペレーティングシステムなどが実際の処理の一部又は全部を行い、その処理によって前記した実施態様の機能が実現される場合も含まれることは言うまでもない。

【0132】更に、記憶媒体から読み出されたプログラムが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わる不揮発性あるいは揮発性の記憶手段に書き込まれた後、そのプログラムの指示に基づき、機能拡張ボードあるいは機能拡張ユニットに備わる演算処理装置などが実際の処理の一部あるいは全部を行い、その処理により前記した実施態様の機能が実現される場合も含まれることは当然である。

【0133】

【発明の効果】本発明によって、このセキュリティ面が向上したことによる、より有効性のあるカード決済を行う決済システム及び方法が可能となった。

【0134】更に携帯端末／ユーザ端末を用いた場合、従来はカードリーダーとカード会社とのカード決済用の情報処理システムを変更する必要があったが、本発明を用いることによって、従来のカードリーダーに無線通信とデータ復号化のユニットを単に接続するのみで、カードリーダーとカード会社とのカード決済用の情報処理システムについては何らの変更を加える必要性がない。従って、カード決済用の情報処理システムの変更の手間負担、コスト負担を回避することが可能となる。

【図面の簡単な説明】

【図1】 本発明のシステム構成の一例を示すシステム構成図である。

50 【図2】 本発明の他のシステム構成の一例を示すシス

テム構成図である。

【図3】 本発明のプロセスの流れの一例を示すフロー
チャート図である。

【図4】 本発明のプロセスの流れの一例を示すフロー
チャート図である。

【図5】 本発明のプロセスの流れの一例を示すフロー
チャート図である。

【図6】 本発明のプロセスの流れの一例を示すフロー
チャート図である。

【図7】 本発明のプロセスの流れの一例を示すフロー
チャート図である。

【図8】 本発明のプロセスの流れの一例を示すフロー
チャート図である。

【図9】 認証画面の一例を示す図である。

【図10】 購入意思確認画面の一例を示す図である。

【図11】 与信拒否画面の一例を示す図である。

【図12】 完了画面の一例を示す図である。

【符号の説明】

* 1 : 決済システム

2 : 認証手段

3 : 第一暗号化手段

4 : ダウンロード手段

5 : 与信判定手段

6 : 会員データベース

7 : 携帯端末

8 : 第二暗号化手段

9 : 無線通信手段A

10 10 : リアル加盟店端末

11 11 : 無線通信手段B

12 12 : 第二復号化手段

13 13 : 第一復号化手段

14 14 : カードリーダー

15 15 : ネットワーク

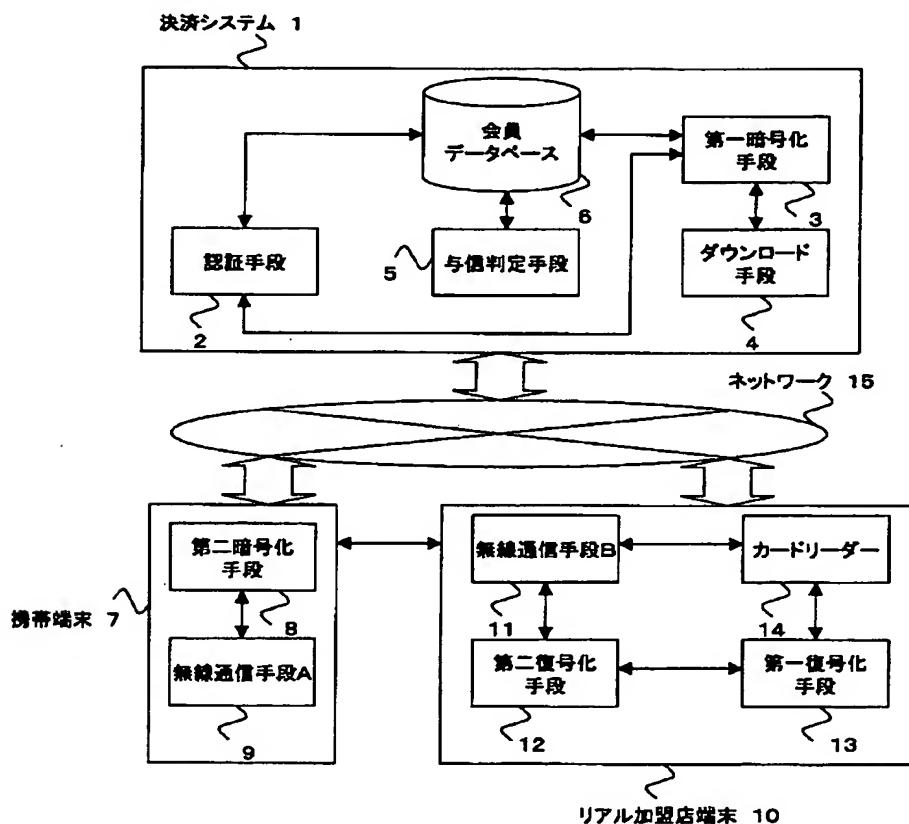
16 16 : カード情報処理手段

17 17 : バーチャル加盟店端末

18 18 : ユーザ端末

*

【図1】



【図9】

認証画面	
パスワード:	
<input type="text"/>	
OK	

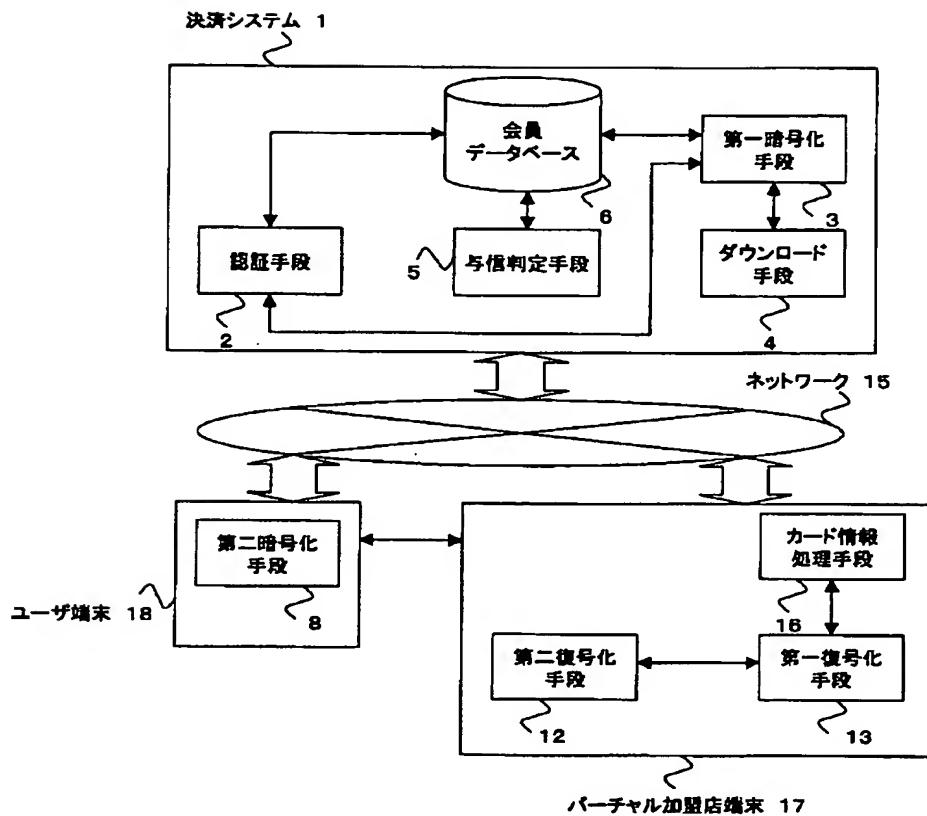
【図10】

購入意思確認画面	
支払いますか？	
<input type="button" value="送信"/>	<input type="button" value="キャンセル"/>

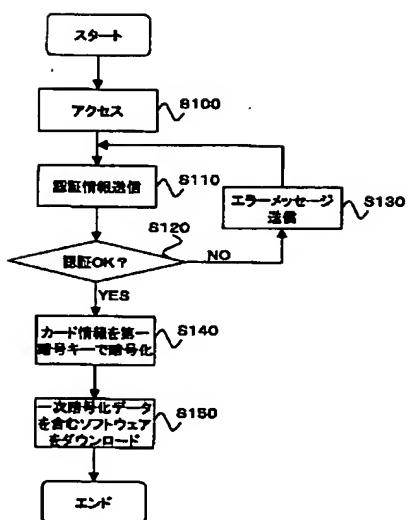
【図11】

与信拒否画面	
カード決済が拒否されました。	

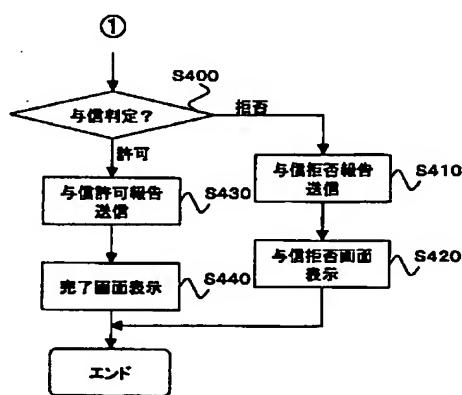
【図2】



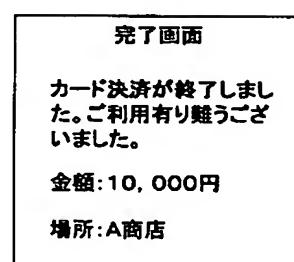
【図3】



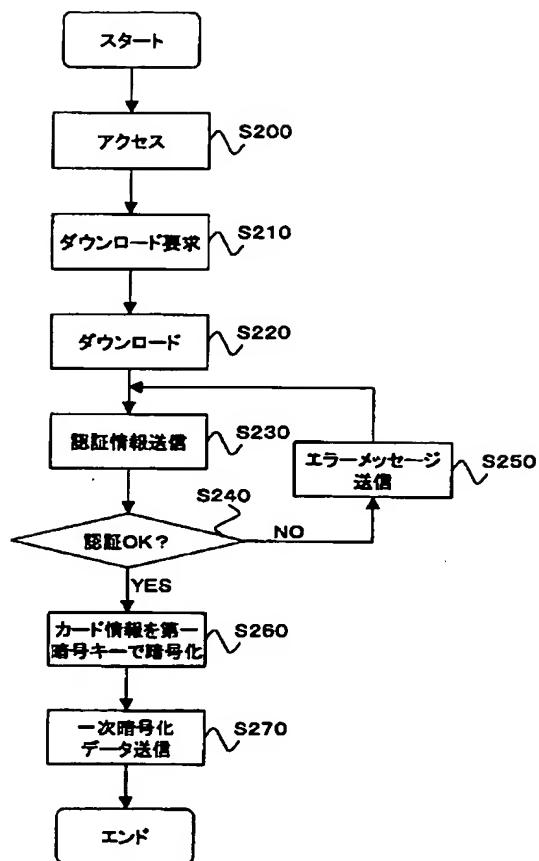
【図6】



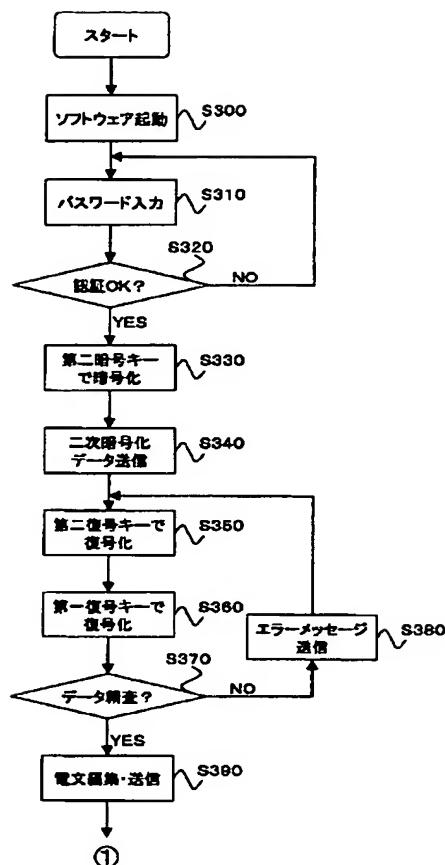
【図12】



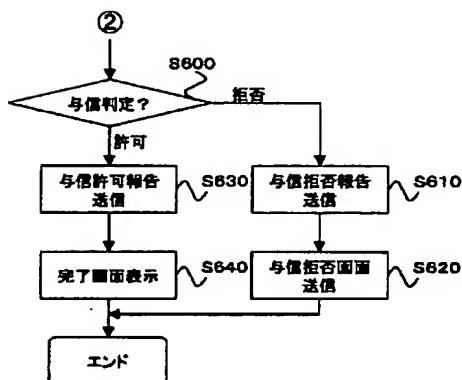
【図4】



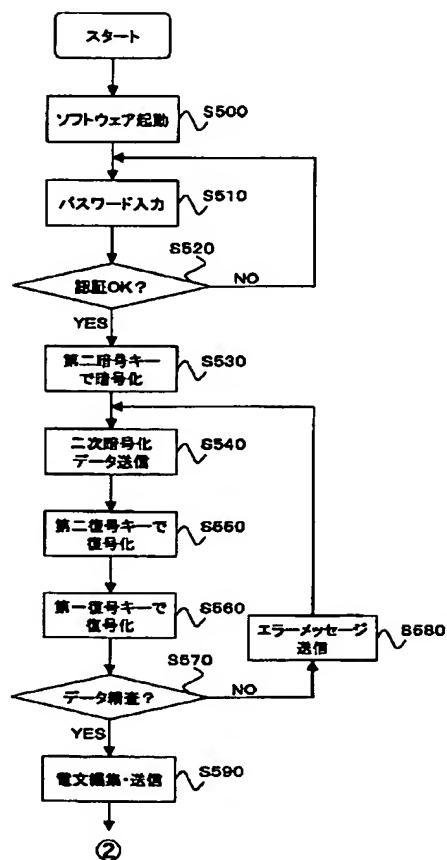
【図5】



【図8】



【図7】



フロントページの続き

(51)Int.Cl.'

G 09 C 1/00

識別記号

6 6 0

F I

G 09 C 1/00

テーマコード(参考)

6 6 0 A

6 6 0 C